UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/748,773	12/30/2003	Willard M. Wiseman	42P17259	8213

8791 7590 07/13/2007

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
TURCHEN, JAMES R	
ART UNIT	**PAPER NUMBER**
2139	

MAIL DATE	DELIVERY MODE
07/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/748,773	WISEMAN ET AL.	
	Examiner	Art Unit	
	James Turchen	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 April 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *04/30/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-28 are pending.

Response to Arguments

Applicant's arguments filed 04/27/2007 have been fully considered but they are not persuasive. Devanbu discloses requesting a service for a platform (the platforms used in the background of the invention being Java (column 2 lines 17-20) or ActiveX (column 3 lines 50-51)). It is inherent that a given platform has at least one configuration. Devanbu discloses certifying the service for execution on the platform, therefore, Devanbu discloses certifying the use of the service for one or more acceptable configurations a the platform. The TLS Protocol was brought into the rejection of claim 1 to make up for Devanbu lacking the limitation "receiving a session key for a session of the service." The TLS Protocol states that symmetric cryptography is used for data encryption. The keys for this symmetric encryption are generated uniquely for each connection (session key) and are based on a secret negotiated by another protocol (such as the TLS Handshake Protocol) (Introduction). Devanbu in view of The TLS Protocol teaches all of the limitations of claim 1. Thus, claims 8, 13, 16, 23 and 26 are also rejected. For claims 12 and 15, rejected as being unpatentable over Devanbu and The TLS Protocol further in view of Klayh, the arguments are non-persuasive. Klayh does not disclose certifying application, but Klayh does disclose selecting from a list of value sets and sending/receiving a confirmation regarding a chosen configuration ("If the server cannot use the context (configuration) provided by the client, it sends its own context negotiation packet back to the client with its preferred

settings. If the client agrees with these settings, it sends an acknowledgement.") Therefore, Klayh is merely used for the purpose of disclosing that selecting from a list of value sets and sending a confirmation is known in the art at the time of invention.

Applicant's arguments, in regards to Devanbu and the TLS Protocol in view of Todd have been fully considered and are persuasive, however, Devanbu discloses sending a certification request and receiving hash data relating to one or more configurations (column 5 line 66-column 6 line 17, generates a message digest (hash) from the data and encrypting it to be used as the signature). The rejection for claims 11, 14 and 27 still stand. Claim 28 was rejected as being unpatentable over Devanbu, The TLS Protocol, and Todd as applied to claim 27, and further in view of Klayh. Claim 27 is still disclosed by Devanbu and The TLS Protocol after the removal of the Todd reference. Thus, claim 28 is rejected as unpatentable under Devanbu and The TLS Protocol as applied to claim 27, and further in view of Klayh as discussed above for claims 12 and 15.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-11, 13, 14, and 16-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Devanbu et al. (6,148,401) and *The TLS Protocol.*

Regarding claims 1, 8, 16, 23, and 26:

Devanbu discloses requesting a service for a platform (the platforms used in the background of the invention being Java (column 2 lines 17-20) or ActiveX (column 3 lines 50-51)). It is inherent that a given platform has at least one configuration. Devanbu discloses certifying the service for execution on the platform, therefore, Devanbu discloses certifying the use of the service for one or more acceptable configurations a the platform. Devanbu et al. does not disclose receiving a session key for a session of the service. The TLS Protocol states that symmetric cryptography is used for data encryption. The keys for this symmetric encryption are generated uniquely for each connection (session key) and are based on a secret negotiated by another protocol (such as the TLS Handshake Protocol) (Introduction). It is inherent to store computer operations that instruct the processor in a tangible form of machine-readable medium.

It would have been obvious to one of ordinary skill in the art to combine the certifying method and system of Devanbu et al. with the method and system of *The TLS Protocol* to ensure session privacy (Introduction).

Regarding claims 2- 5, 9, 10, and 17-20:

Devanbu et al. discloses a method and system for the use of a public key system, but it does not disclose having an identifying credential comprising of an identity key. *The TLS Protocol* discloses a method and system for authenticating a peer using

"asymmetric, or public key, cryptography" (Introduction). A certification authority (CA) is a characteristic of many public key infrastructures and the CA attests that a particular key belongs to a particular client/server (section F). A public key is made public by a CA and is a trusted third party. The identification credential that would be received from the service provider is disclosed in *The TLS Protocol* as being a temporary RSA key. It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method and system for the use of a public key system Devanbu et al. with the authentication system and method of *The TLS Protocol* in order to incorporate authenticating a client/server (Introduction).

Regarding claims 6, 21, and 24:

Devanbu et al. discloses the method and system receiving and sending a program that has been certified to one or more configurations (column 4 lines 25-52), but it does not disclose using a hash function. *The TLS Protocol* discloses using a secure hash function (SHA, MD5, etc.) to ensure the connection is reliable and that the data is unmodified (Introduction). It would have been obvious to one of ordinary skill in the art at the time of invention to combine the method and system of sending and receiving a certified program of Devanbu et al. with the method and system of using a hash function in order to ensure a reliable connection (*The TLS Protocol* – Introduction).

Regarding claims 7, 22, and 25:

Devanbu et al. discloses a method and system for certifying the use of the program (service) comprises confirming that a chosen configuration is included in a set of values representing the one or acceptable configurations (Figure 6).

Regarding claims 11, 14, and 27:

Devanbu discloses sending a certification request and receiving hash data relating to one or more configurations (column 5 line 66-column 6 line 17, generates a message digest (hash) from the data and encrypting it to be used as the signature)

Regarding claim 13:

Devanbu et al. discloses a communication device to communicate with a service provider (figure 7) and a trusted platform module (column 4 lines 25-52). Devanbu et al. also discloses the client device providing assurance to the service provider that the service is limited to on or more acceptable configurations (column 4 lines 25-52).

Claims 12, 15, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Devanbu et al and *The TLS Protocol* as applied to claims 8, 13, and 27 above, and further in view of Klayh (WO/2000/038089).

Regarding claims 12 and 15:

Devanbu et al. and *The TLS Protocol* disclose all of the limitations of claims 8 and 13, but they do not disclose choosing from a list of received value sets to the one or more acceptable configurations and sending a confirmation that a chosen configuration is included in the list of acceptable value sets. Klayh discloses choosing a configuration and sending a confirmation that a configuration has been chosen (page 8). It would have been obvious to one of ordinary skill in art at the time of invention to combine the method and system disclosed in claims 8 and 13 with the confirmation system disclosed by Klayh in order to determine whether the configuration is acceptable (page 8).

Regarding claim 28:

Devanbu et al and *The TLS Protocol* disclose all of the limitations of claim 27, but they do not disclose choosing from a list of received value sets to the one or more acceptable configurations and sending a confirmation that a chosen configuration is included in the list of acceptable value sets. Klayh discloses choosing a configuration and sending a confirmation that a configuration has been chosen (page 8). It would have been obvious to one of ordinary skill in art at the time of invention to combine the system disclosed in claim 27 with the confirmation system disclosed by Klayh in order to determine whether the configuration is acceptable (page 8).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Turchen whose telephone number is 571-270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JRT

TAGHI ARANI
PRIMARY EXAMINER
7/5/07